UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,133	01/16/2001	Ernest S. Richards	909-1	3427

7590 01/26/2005

Michael F. Petock, Esquire
46 The Commons at Valley Forge
1220 Valley Forge Road
Post Offuce Box 856
Valley Forge, PA 19482-0856

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/761,133	RICHARDS, ERNEST S.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to application filed on January 01, 2001. Original application contained Claims 1-37. Therefore, Claims 1-37 are pending for consideration.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

1. Claims 1-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (EPA EP 0770 953 A2).

2. Regarding claim 1 Fischer teaches and describes a method of electronically verifying [notarizing] that a person possessing a security device is who the person claims to be (col.1 line 35 to col.2 line 7), comprising (Fig.1):

sending a message by said security device [trusted device, such as smart card, notary decoder, smart card disk or MCIA device] associated with the person whose identity is to be

verified, said message including said person's public key number (col.7 line 10 to line 22, acol.7 line 26 to line 33);

receiving said message by a host, said host encrypting a random message using said public key number and sending said public key number encrypted message to said security device (col.7 line 26 to line 45);

said security device decrypting said public key number encrypted random message using said person's private key number and sending said decrypted random message to said host (col.6 line 56 to col.7 line 10); and

said host comparing the decrypted random message sent by the security device with the random message previously encrypted by said host with said public key number to verify the identity of the person (col.7 line 41 to line 55).

3. Regarding claim 22 Fischer teaches and describes a apparatus for enabling electronic identification of a person, comprising:

means for permanently storing a corresponding private key number and a public key number assigned to said person;

means for sending said public key number to a host seeking to verify the identity of said person (col.7 line 10 to line 22, acol.7 line 26 to line 33);

means for receiving from said host a random message encrypted with said public key number (col.7 line 26 to line 45);

means for decrypting said random message encrypted with said public key number (col.6 line 56 to col.7 line 10); and

means for sending said decrypted random message to said host for comparison to said random message previously encrypted with said public key number to verify the identity of said person (col.7 line 41 to line 55).

4. Claims 2-3, 8, 9, 18, and 19 are rejected applied as above in rejecting Claim 1. Furthermore, Fischer teaches and describes a method to identify and verify that a party utilizing a piece of electronic equipment, such as a personal computer on the Internet, is who he or she claims to be, wherein:

As to claim 2, said security device is a computer with associated security hardware having said person's private key number programmed therein (col.4 line 1 to line 3m and col.4 line 9 to line 13).

As to claim 3, said security device is a laptop computer with associated security hardware having said person's private key number programmed therein (col.2 line 9 to line 16).

As to claim 8, said security device is a computer provided with associated security software having said person's private key number programmed therein (col.4 line 1 to line 3, and col.4 line 9 to line 25).

As to claim 9, said security device is a laptop computer provided with associated security software having said person's private key number programmed therein (col.2 line 9 to line 16, and col.8 line 54 to col.9 line 1).

As to claim 18, said host first sends a query to said security device as to its identity before said security device sends a message which includes said person's public key number (col.7 line 3 to line 10, col.8 line 5 to line 11, and col.10 line 17 to line 32).

As to claim 19, the method of electronically verifying is repeated during a session on which said security device is logged-on to said host (col.8 line 27 to line 40, and col.14 line 30 to line 34)

5. Claims 23, and 27-31 are rejected applied as above in rejecting Claim 22. Furthermore, Fischer teaches and describes an apparatus to identify and verify that a party utilizing a piece of electronic equipment, such as a personal computer on the Internet, is who he or she claims to be, wherein:

As to claim 23, including means at said host for generating a random message (col.4 line 34 to line 47, col.7 line 41 to line 47).

As to claim 27, said means for decrypting said random message includes use of the RSA algorithm (col.4 line 18 to line 25).

As to claim 28, said means for permanently storing is comprised of a one time programmable microprocessor (col.3 line 58 to col.4 line 3, and col.4 line 9 to line 18).

As to claim 29, said means for permanently storage comprises a read only memory (col.3 line 58 to line 59).

As to claim 30, said apparatus is contained on security hardware which communicates with a computer (col.3 line 55 to col.4 line 3, and col.4 line 9 to line 18).

As to claim 31, said computer is a laptop computer (col.2 line 9 to line 16).

As to claim 36, said apparatus is mounted on a card for use as a financial transaction card [smart card](col.3 line 49 to line 54).

As to claim 37, said apparatus is mounted on an identification card [such as smart card] (col.3 line 49 to line 54).

6. Claims 4-7, 10-11, and 20-21are rejected applied as above in rejecting Claims 2, 3, and 19. Furthermore, Fischer teaches and describes a method to identify and verify that a party utilizing a piece of electronic equipment, such as a personal computer on the internet, is who he or she claims to be, wherein:

As to claim 4, said security hardware includes a one time Programmable macroprocessor (col.3 line 58 to col.4 line 3, and col.4 line 9 to line 18).

As to claim 5, said security hardware includes a one time programmable microprocessor (col.3 line 58 to col.4 line 3, and col.4 line 9 to line 18).

As to claim 6, said security hardware includes a read only memory for storing said person's private key number (col.3 line 58 to line 59).

As to claim 7, said security hardware includes a read only memory for storing said person's private key number (col.3 line 58 to line 59).

As to claim 10, said security hardware is insertable and removable in a drive of said computer (col.10 line 33 to line 43).

As to claim 11, said security hardware is insertable and removable in a drive of said laptop computer (col.3 line 49 to line 54,and col.10 line 33 to line 43).

As to claim 20, said repeated verification is invisible [executing on computer] to said person possessing said security device (col.8 line 27 to line 40, and col.14 line 30 to line 34).

As to claim 21, said host compartmentalizes [executed separately] data requiring a verification for each data compartment (col.14 line 35 to line 44).

7. Claims 24-26 are rejected applied as above in rejecting Claims 23, and 30. Furthermore, Fischer teaches and describes a method and apparatus to identify and verify that a party utilizing a piece of electronic equipment, such as a personal computer on the internet, is who he or she claims to be, wherein

As to claim 24, including means at said host for encrypting said random message (col.7 line 26 to line 45).

As to claim 25, said random message is a random number (col.4 line 35 to line 47).

As to claim 26, said means at said host for encrypting includes use of the RSA algorithm (col.4 line 18 to line 25).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 12-17, and 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (EPA EP 0770 953 A2) and further in view of DeLaHuerga (U. S. Patent 6,779,024).

2. Claims 12-17, and 34-35 are rejected applied as above in rejecting claim 1, and 22. Furthermore, regarding Claim 12-17, and 34-35 Fischer teach and describe a method of identification and comprising, a personal identification apparatus embodied in a token device such as a smart card. The portable identification (notary) device includes an input/output port, which is coupled to a single integrated circuit chip. The I/O port is coupled to a conventional smart card reading device which in turn is coupled to a PC, laptop computer or similar devices. A tamper resistant secret private key storage is embodied on the chip. The private key storage is coupled to a processor which, in turn, is coupled to a permanent memory that stores the program executed by the processor, and a random value generator are also preferably coupled to the host processor (Fig.1, abstract, col.2 line 9 to line 26).

Although the system disclosed by Fischer shows all the features of the claimed limitation, but Fischer does not specifically disclose other forms of identification device, such as badge, car key, and other mode of connecting the identification device to host (certification node), such as wireless communication.

In an analogous art, DeLaHuerga, on the other hand disclose computing environment that relates to system and methods which provide a wireless communication options, such as radio frequency link and infrared link using badge (or car key card) to authenticate and send and receive transaction from an identification device to a host such as certifier (abstract, col9 line8 to line 57).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Fischer and DeLaHuerga, because DeLaHuerga's method of communication of different identification device(s) by using wireless communication would not only extend and enhance the input/output option of identification device, such as secure badges, in the system of Fischer during transmitting and receiving data from host server but will also provide other portable options to customize user identification services.

As to claim 12, said security device is a badge or identification card (DeLaHuerga: col.19 line 13 to line 30) with associated security hardware having said person's private key number programmed therein (Fischer: col.4 line 1 to line 3, and col.4 line 9 to line 25).

As to claim 13, said security device is a car key (DeLaHuerga: col.19 line 13 to line 30) with associated security hardware having said person's private key number programmed therein (Fischer: col.4 line 1 to line 3, and col.4 line 9 to line 25).

As to claim 14, said security hardware (Fischer: Fig.1) communicates with a computer by an infrared link (DeLaHuerga: col.18 line 44 to line 58).

As to claim 15, said security hardware Fischer: Fig.1) communicates with a computer by a radio frequency link (DeLaHuerga: col.18 line 44 to line 58).

As to claim 16, said security hardware Fischer: Fig.1) communicates with a laptop computer by an infrared link (DeLaHuerga: col.18 line 44 to line 58).

As to claim 17, said security hardware communicates with a laptop computer by a radio frequency link (DeLaHuerga: col.19 line 13 to line 30).

As to claim 34, said apparatus is mounted on a badge (DeLaHuerga: col.19 line 13 to line 30).

As to claim 35, said apparatus is mounted on a card for use as a car key (DeLaHuerga: col.19 line 13 to line 30).

3. Claims 32, and 33 1are rejected applied as above in rejecting Claim 30. Furthermore, Fischer teaches and describes a method and apparatus to identify and verify that a party utilizing a piece of electronic equipment, such as a personal computer on the Internet, is who he or she claims to be, wherein:

As to claim 32, said security hardware Fischer: Fig.1) communicates with said computer by an infrared link key (DeLaHuerga: col.19 line 13 to line 30).

As to claim 33, said security hardware Fischer: Fig.1) communicates with said computer by a radio frequency link key (DeLaHuerga: col.19 line 13 to line 30).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please refer attached PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ
December 30, 2004